Wisacwis
County Interfaces

VPN Client Installation and Configuration Guide

Overview

The VPN client is used to establish a secure connection to the DHFS network. If your county needs to access additional county servers (database, MQSeries etc) while the VPN connection to DHFS is running then a “split-tunnel” vpn group should be setup. Otherwise, the default “DHFSNT” group may be used – this group makes the county network “invisible” while connected to the DHFS network.

Please contact you Wisacwis Technical Representative to discuss these issues and determine your needs. (This discussion will probably require input from a county network specialist and DHFS network specialist to determine exact needs and requirements.)

Firewall Changes

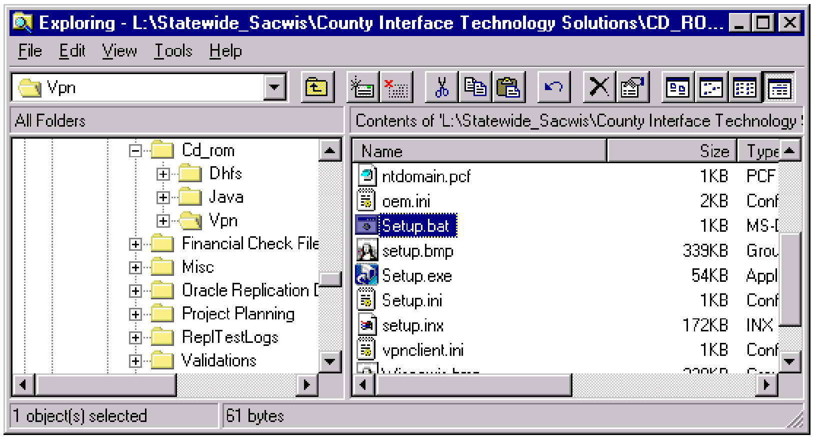
In order to establish a VPN connection to DHFS, you will need to make a few changes on your firewall (assuming that the proper traffic is not already allowed into your network). The VPN tunnel is created using IPSec, which is implemented with two core Transport Layer protocols: 1) Authentication Header (AH, protocol 51) and 2) Encapsulating Security Payload (ESP, protocol 50). In addition to these two, the Application Layer protocol, Internet Security Association and Key Management Protocol (ISAKMP, UDP port 500) is also used for key exchanges. We are using a Cisco VPN concentrator, and Cisco uses UDP port 10000 as a way to get around NAT/PAT problems associated with IPSec tunnels (Transparent Tunneling).

The IP address of our VPN concentrator is, 165.189.41.30, so what you will need to do is allow the following from that specific address, and only that address:

protocols 50 and 51
UDP ports 500 and 10000

Even if you do not use any form of NAT or PAT, it will not hurt to include UDP port 10000 in the list. If you find that your firewall product does not allow for a fine-grained control list (e.g. you cannot specify protocol 50 or 51, only TCP, UDP, ICMP, etc.), then you can just put a rule in that allows "All traffic" from our concentrator instead of specifically listing all four of the above entries. It is up to you whether or not you allow this traffic into any part of your network or only to the specific server that will be establishing the VPN tunnel. You only need to allow the traffic to the one machine.

Setup



Exploring - L:\Statewide_Sacwis\County Interface Technology Solutions\CD_RO...

Vpn

Contents of 'L:\Statewide_Sacwis\County Interface Technology S

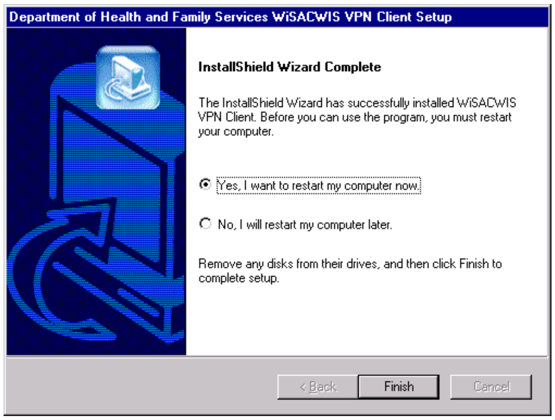
- Cd_rom
  - Dhfs
  - Java
  - Vpn
- Financial Check File
- Misc
- Oracle Replication [
- Project Planning
- ReplTestLogs
- Validations

Name	Size	Type
ntdomain.pcf	1KB	PCF
oem.ini	2KB	Conf
Setup.bat	1KB	MS-[
setup.bmp	339KB	Grou
Setup.exe	54KB	Appl
Setup.ini	1KB	Conf
setup.inx	172KB	INX
vpnclient.ini	1KB	Conf

1 object(s) selected | 61 bytes

Run the **setup.bat (**not the setup.exe).

Wait while the required files are installed …



Department of Health and Family Services WiSACWIS VPN Client Setup

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed WiSACWIS VPN Client. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Upon completion of the install select “Yes, I want to restart my computer now” and click finish button to proceed.

VPN Client Network Placement

There are two possible scenarios when placing the VPN client machine on your network.

1) You could have the VPN client machine on the same class C network as any other machines that it needs to communicate with while a VPN session is established (e.g. Database servers). For example, if the VPN client machine were assigned an IP address of 10.0.1.5, and a database server that needs to communicate with the VPN machine had an IP address of 10.0.1.10, then they would be on the same class C network.
2) The VPN client machine is on a different network than other machines that need to communicate with it. An example would be, the VPN machine has an IP address of 10.0.1.5, and a database server has an IP address of 172.16.5.22.

Important:

If you are going to place your VPN client machine as described in scenario 1 above, then you can use the existing Connection Entry that comes pre-configured with the VPN client after one simple modification. Go to the section entitled, "Modifing the Existing Connection Entry", and skip the next section entitled, "Creating a New Connection Entry".

If you are going to place your VPN client machine as described in scenario 2 above, then you will need to contact your Wisacwis technical contact prior to implementation and provide the following information:

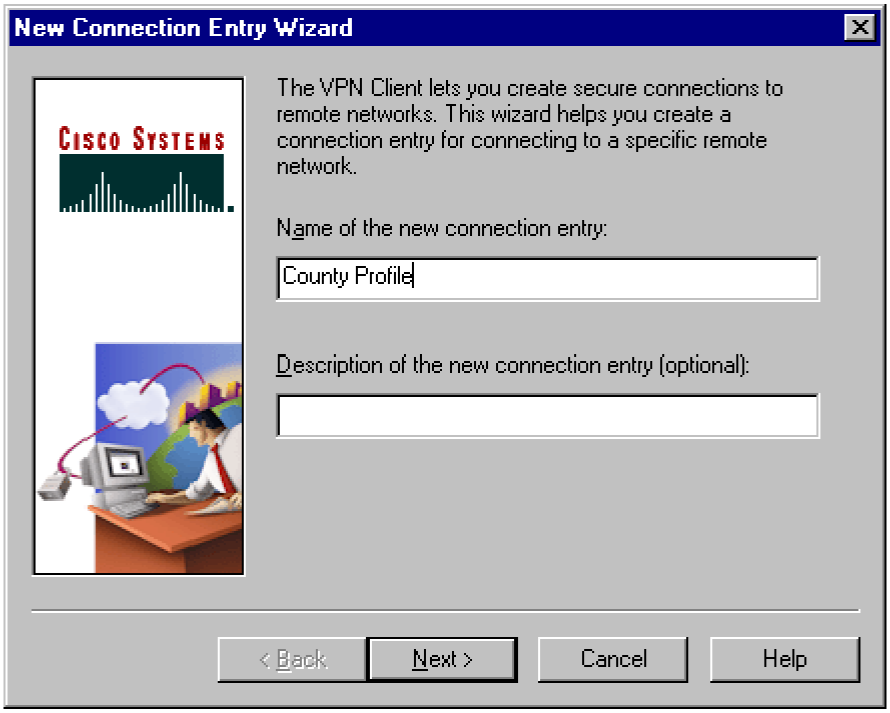
1. The IP network that your database server is on (e.g. 172.16.5.0).
2. Any other networks with machines on them that need to communicate with the VPN client machine while a VPN session is established. For instance, you may need a management machine or monitoring machine such as a HP Openview station to communicate with the VPN client machine.

You should also ask for the password for your customized VPN group as well, which will be used later when configuring a new Connection Entry. DHFS staff assigns this password once they are notified that a new county VPN group is required.

Once you have exchanged all of the necessary information, go on to the next section entitled, "Creating a New Connection Entry".

Creating a New Connection Entry

For a custom VPN group, create a new Connection Entry by clicking on New from the first screen presented to you after running the VPN client. Enter a name and description – the name should be one word eg “DaneProfile”. Remember the name you chose; you will need it again.



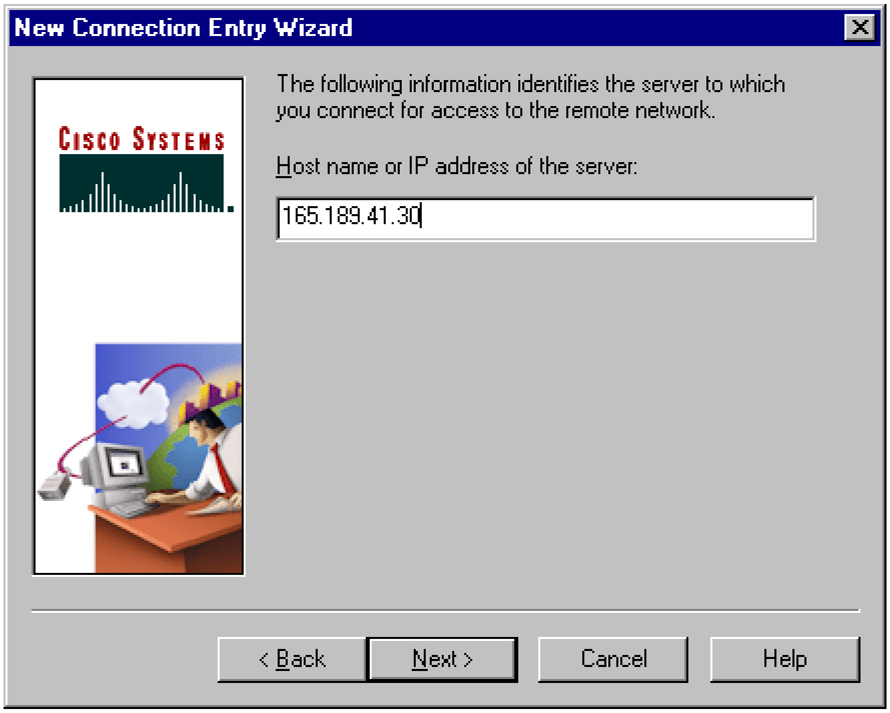
New Connection Entry Wizard

The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.

Name of the new connection entry: County Profile

Description of the new connection entry (optional):

After clicking on Next, you will be prompted for the IP address of the DHFS VPN server. Enter: 165.189.41.30 as shown below.

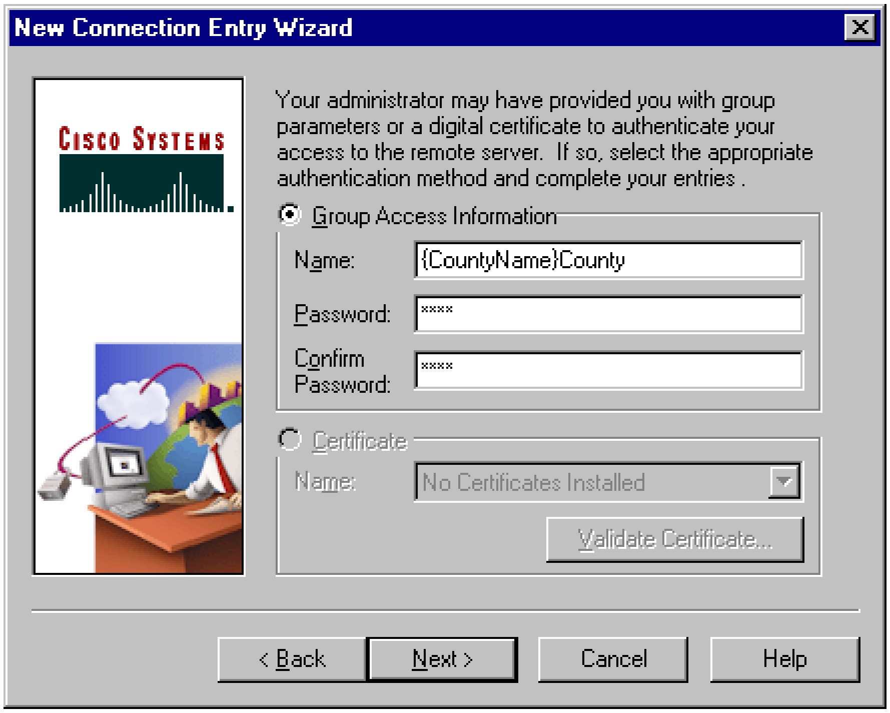


New Connection Entry Wizard

The following information identifies the server to which you connect for access to the remote network.

Host name or IP address of the server: 165.189.41.30

Click on Next, then you will be prompted for a group name and a Password. Your group Name is going to be your county, followed by the word, "County". For example, instead of {CountyName}County as is shown in the picture below, Dane County's Name would be DaneCounty (no spaces). Please contact your Wisacwis technical representative to get the password for your VPN group.



New Connection Entry Wizard

Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .

● Group Access Information

Name: {CountyName}County

Password: ****

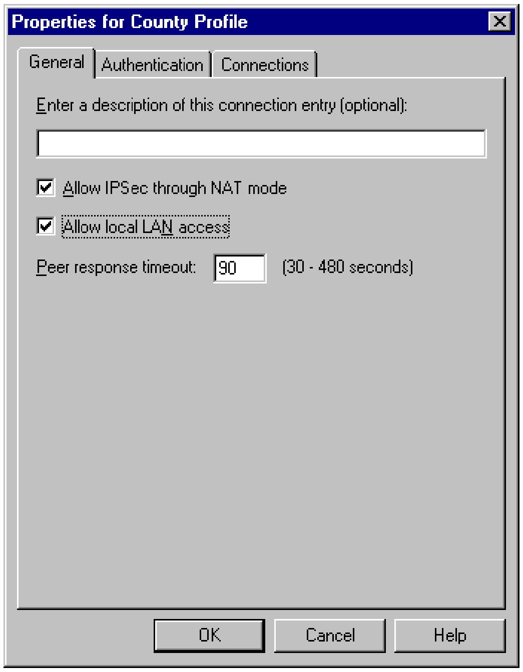
Confirm Password: ****

○ Certificate

Name: No Certificates Installed

Click on Next, then click on Finish when prompted to continue.

Now you just need to make one more change for that Connection Entry before it's ready to use. Make sure the new entry is selected in the Connection Entry list, then click on Options*Properties. Different versions of the client look slightly different, but you should see a check box similar to Allow local LAN access. Make sure that is checked, then click OK.



Enter a description of this connection entry (optional):

☑ Allow IPSec through NAT mode

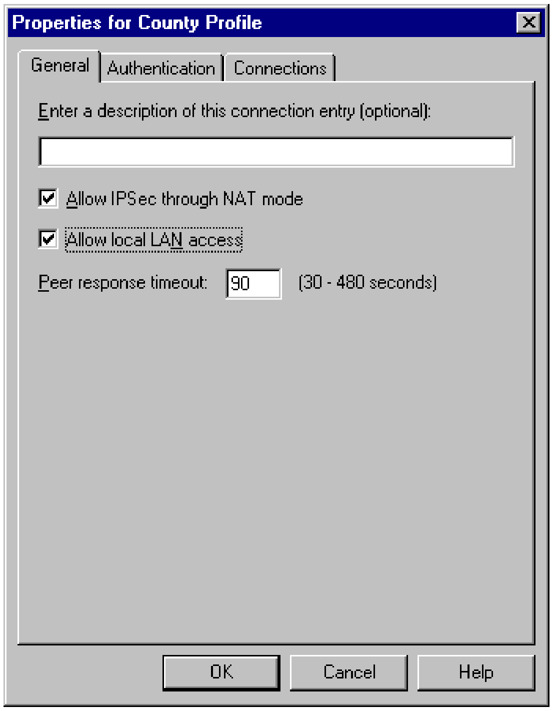
☑ Allow local LAN access

Peer response timeout: 90 (30 - 480 seconds)

Modifying the Existing Connection Entry

From the initial screen presented after running the VPN client, click on Options*Properties. Different versions of the client look slightly different, but you should see a check box similar to Allow local LAN access. Check this box, then click on the Authentication tab.

Change the Name from "ntdomain" to "split". The password should be the same. If there seems to be a problem connecting, contact your Wisacwis technical contact to verify the configuration.

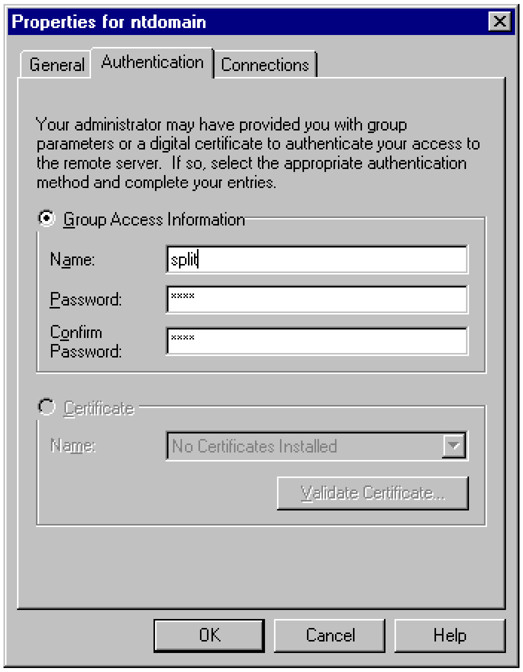

Properties for County Profile

Enter a description of this connection entry (optional):

☑ Allow IPSec through NAT mode

☑ Allow local LAN access

Peer response timeout: 90 (30 - 480 seconds)


Properties for ntdomain

Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries.

● Group Access Information

Name: split

Password: ****

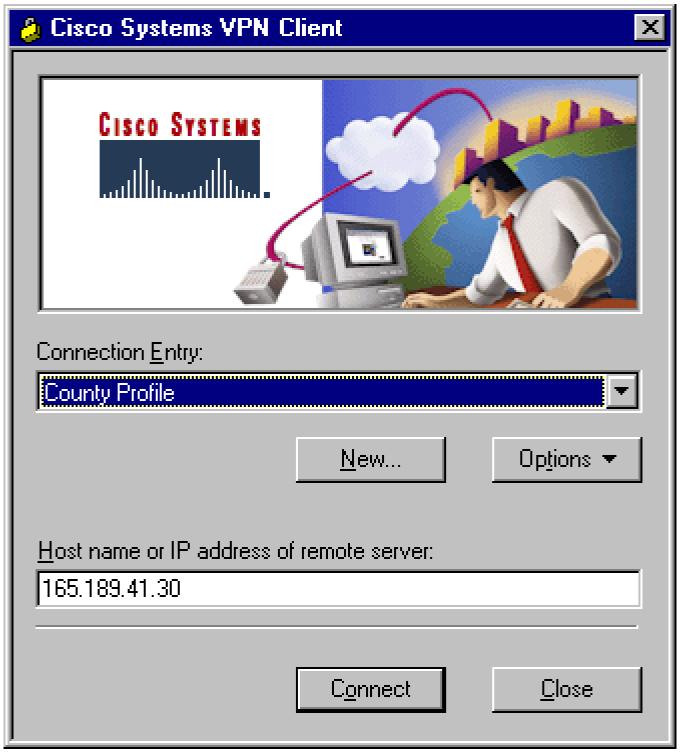
Confirm Password: ****

○ Certificate

Name: No Certificates Installed

Test the VPN Connection

Select from Start menu: Programs*VPN Client*Wisacwis VPN Connect

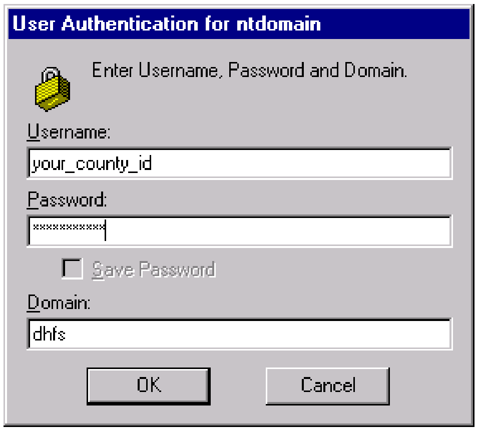


Cisco Systems VPN Client

Connection Entry: County Profile

Host name or IP address of remote server: 165.189.41.30

Select the appropriate Connection Entry, then click the Connect button. You should be prompted for your VPN username and password, enter those in the User Authentication dialog, then click OK to establish the connection. This username is associated with a different account than the group Name used above, though the actual name itself may be the same as the group Name. The format is, {CountyName}County. So Dane county would have a username of, DaneCounty (case does not matter, this is capitalized for emphasis). The password is different than the group password from above as well, so again, contact your Wisacwis Technical contact to make sure you have that.



User Authentication for ntdomain

Enter Username, Password and Domain.

Username: your_county_id

Password: ***********

□ Save Password

Domain: dhfs

If everything works properly, you should see a yellow lock appear in your system tray (bottom right corner of your desktop). In order to make sure that you can properly communicate with both the DHFS network, and your own local network, do the following:

1) To test network connectivity on the DHFS LAN, ping the DNS server at DHFS by IP address. Type the following from a command prompt:

    ```
    Ping 159.158.53.9
    ```

2) To test DNS functionality, ping the DNS server by its name, dhfs-dns.dhfs.state.wi.us. You should see something similar to this:

```
C:\>ping dhfs-dns.dhfs.state.wi.us

Pinging dhfs-dns.dhfs.state.wi.us [159.158.53.9] with 32 bytes of data:

Reply from 159.158.53.9: bytes=32 time<10ms TTL=126
Reply from 159.158.53.9: bytes=32 time<10ms TTL=126
Reply from 159.158.53.9: bytes=32 time<10ms TTL=126
Reply from 159.158.53.9: bytes=32 time<10ms TTL=126
```

3) Try pinging another machine on the same Class C network as the VPN client by IP address. For example, if your VPN client machine has an IP address of 10.0.1.5, try pinging your default gateway, which is likely, 10.0.1.1.

If you are using the "split" group, as described in the "Modify the Existing Connection" section above, you can stop here. The connection is ready to go. If, however, you are using a custom group, as described in the "Create a New Connection Entry" section above, then you should also do the following tests.

4) Try pinging your db server, or any machine on one of the "allowed" networks (as was communicated to your Wisacwis technical contact). Be sure to use the IP address, not the DNS name for that machine.
5) If you need to be able to establish a connection or communicate with the VPN machine **from** another machine on an "allowed" network (rather than from the VPN machine **to** that other box), then you should also go to that machine and try pinging the local IP address of the VPN machine as well.

Automating VPN Login

To prevent the “User Authentication” dialog from popping up when establishing a connection, the VPN profile can be altered to save the user information and automatically provide it.

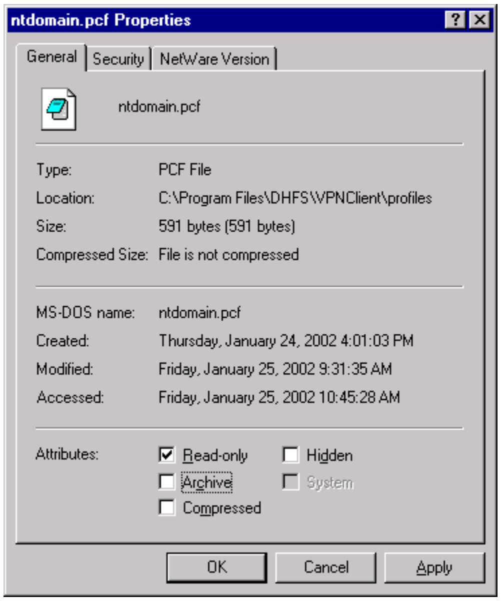
Edit the vpn profile located in C:\Program files\DHFS\VPNClient\profiles\ntdomain.pcf

(If a custom .pcf file is being used to allow split-tunneling then edit it instead.)

Change the following : (**DO NOT ALTER ANY OTHER VALUES**)

Username=*your username*
SaveUserPassword=1
UserPassword=*your password*

Save the profile then set its **read-only** attribute via the file properties dialog. (Right click the profile and select Properties option from the popup menu.) If the profile is not set to read-only then the next time a connection is established the VPN client will reset the values that were altered and the User Authentication dialog will prompt for the information.



ntdomain.pcf

Type: PCF File
Location: C:\Program Files\DHFS\VPNClient\profiles
Size: 591 bytes (591 bytes)
Compressed Size: File is not compressed

MS-DOS name: ntdomain.pcf
Created: Thursday, January 24, 2002 4:01:03 PM
Modified: Friday, January 25, 2002 9:31:35 AM
Accessed: Friday, January 25, 2002 10:45:28 AM

Attributes: ☑ Read-only ☐ Hidden
☐ Archive ☐ System
☐ Compressed

Test these changes by running “Wisacwis VPN Connect” – the User Authentication dialog should not appear. Disconnect, then verify that the profile changes that were made have not been reset.